AMENDMENTS TO THE CLAIMS

Please add or amend the claims to read as follows, and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application claims indicated as cancelled:

1. (**Currently Amended**) A method performed by a server processor comprising:
responding, by the server processor, to a contact point created by a party ~~committing fraud~~, the response including a set of details, the set of details including a set of false personal information, said false personal information including information associated with a false account;
monitoring said false account for attempted access; and
based on an attempt to access said false account, determining that said party is attempting to commit fraud.

2. (**Currently Amended**) The method of claim 1, comprising responding to [[a]] said contact point a plurality of times, each response including a different set of details, each said set of details including a respective different set of false account information.

3. (Original) The method of claim 1, wherein the contact point is an Internet address referring to a web site.

4. (Original) The method of claim 1, wherein the contact point is an e-mail address.

5. (Original) The method of claim 1, wherein responding comprises transmitting information at a speed designed to mimic a human entering data.

6. (**Currently Amended**) The method of claim [[1]] 2, comprising setting the timing of the responses to resemble that of a set of users responding to a Phishing attack.

7. (**Currently Amended**) The method of claim [[1]] 2, wherein each of said plurality of responses ~~response~~ includes a set of details that [[are]] is internally consistent.

8. (**Currently Amended**) The method of claim 1, comprising creating a database including a plurality [[set]] of false identities, each false identity including [[a]] an internally consistent set of data ~~which is consistent within the set of data~~.

9. (**Currently Amended**) The method of claim [[1]] 2, wherein each of said plurality of responses ~~response~~ includes a respective set of details consistent with an Internet service provider used to respond.

10. (**Currently Amended**) The method of claim 1, wherein the responding is in response to [[a]] an email Phishing attack, wherein the contact point is transmitted by email.

11. (**Currently Amended**) The method of claim [[1]] 2, wherein the responding is conducted for the plurality of responses using a respective plurality of Internet access points.

12. (**Currently Amended**) The method of claim [[1]] 2, wherein the responding is conducted for the plurality of responses using a respective plurality of intermediate networks.

13. (**Currently Amended**) The method of claim [[1]] 2, wherein the responding is conducted for the plurality of responses using a respective plurality of intermediate Internet service providers.

14. (Original) The method of claim 1, wherein the data in a response is marked, the method comprising monitoring an institution for the use of marked data in an attempted transaction.

15. (Previously Presented) The method of claim 1, wherein the number of responses sent by the server processor is in proportion to a size of an attack in response to which the responses are sent.

16. (Original) The method of claim 1, wherein responding comprises entering data into a web-form.

17. (Original) The method of claim 1, comprising marking a response using a cryptographic algorithm, such that the marking is detectable only with a suitable cryptographic key.

18. (Original) The method of claim 1, wherein the details and the timing of the sending of the data mimic the behavior of automated client software.

19. (Original) A method comprising:

contacting a plurality of times a website and, with each contact, filling in a web-form with a set data, each set of data including a set of details, the set of details including a set of false personal information.

20. (Original) The method of claim 19, wherein filling in the web-form comprises transmitting information at a speed designed to mimic a human entering data.

21. (Original) The method of claim 19, comprising setting the timing of the contacting to resemble that of a set of unrelated users.

22. (Original) The method of claim 19, wherein each contact includes a set of details that are internally consistent.

23. (Previously Presented) The method of claim 19, comprising creating a database including a set of false identities, each false identity including a set of data which is consistent within the set of data.

24. (**Currently Amended**) a system comprising:

a server processor to:

respond to a contact point created by a party ~~committing fraud~~, the response including a set of details, the set of details including a set of false personal information, said false personal information including information associated with a false account;

monitor said false account for attempted access; and

based on an attempt to access said false account, determine that said party is attempting to commit fraud.

25. (Original) The system of claim 24, wherein the contact point is an Internet address referring to a web site.

26. (Original) The system of claim 24, wherein the contact point is an e-mail address.

27. (Original) The system of claim 24, wherein responding comprises transmitting information at a speed designed to mimic a human entering data.

28. (Original) The system of claim 24, wherein the timing of the responses is to resemble that of a set of users responding to a Phishing attack.

29. (**Currently Amended**) The system of claim 24, ~~wherein each response includes a set of details that are internally consistent~~ wherein said server processor is to respond to said contact point a plurality of times, using a plurality of respective sets of internally consistent details, each set of details including a respective set of false personal information, including information associated with a respective false account, wherein said server processor is to monitor said plurality of false accounts for attempted access.

30. (**Currently Amended**) The system of claim [[24]] 29, comprising a database including a set of false identities, each false identity including a set of data which is consistent

within the set of data, wherein said server processor is to respond to the contact point using said sets of false identities.

31. (**Currently Amended**) The system of claim [[24]] 29, wherein the responding is conducted using a plurality of intermediate networks for the plurality of responses respectively.

32. (Original) A system comprising:

a server processor to contact a plurality of times a website and, with each contact, enter a set of data, each set of data including a set of details, the set of details including a set of false personal information.

33. (**Currently Amended**) The system of claim 32, comprising a database including a plurality [[set]] of false identities, wherein the server processor is to contact the website a plurality of times using said plurality of false identities respectively.

34. (Original) The system of claim 32, wherein entering the data comprises transmitting information at a speed designed to mimic a human entering data.